

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of

Implementation of the Telecommunications Act of 1996;

CC Docket No. 96-115

Telecommunications Carriers' Use of Customer
Proprietary Network Information and Other Customer
Information;

Petition for Rulemaking to Enhance Security and
Authentication Standards for Access to Customer
Proprietary Network Information

RM-11277

COMMENTS OF CENTENNIAL COMMUNICATIONS CORP.

Centennial Communications Corp d/b/a Centennial Wireless and its subsidiaries providing telecommunications services¹ (collectively "Centennial"), provide commercial mobile radio service ("CMRS") throughout the United States.² Protecting the privacy of customer information is of utmost importance to Centennial, and Centennial agrees that the Commission should be very concerned about data brokers who masquerade as

¹ The subsidiaries joining in this filing are: Bauce Communications of Beaumont, Inc., Bauce Communications, Inc., Centennial Beauregard Cellular LLC, Centennial Beauregard Holding Corp., Centennial Benton Harbor Cellular Corp., Centennial Benton Harbor Holding Corp., Centennial Caldwell Cellular Corp., Centennial Cellular Operating Company LLC, Centennial Cellular Telephone Company of San Francisco, Centennial Cellular Tri-State Operating Partnership, Centennial Claiborne Cellular Corp., Centennial Clinton Cellular Corp., Centennial Hammond Cellular LLC, Centennial Iberia Holding Corp., Centennial Jackson Cellular Corp., Centennial Lafayette Cellular Corp., Centennial Lafayette Communications LLC, Centennial Louisiana Holding Corp., Centennial Mega Comm Holding Corp., Centennial Michiana License Co. LLC, Centennial Michigan RSA 6 Cellular Corp., Centennial Michigan RSA 7 Cellular Corp., Centennial Morehouse Cellular LLC, Centennial Randolph Cellular LLC, Centennial Randolph Holding Corp., Centennial Southeast License Company LLC, Century Beaumont Cellular Corp., Century Cellular Realty Corp., Century Elkhart Cellular Corp., Century Indiana Cellular Corp., Century Michiana Cellular Corp., Century Michigan Cellular Corp., Century Southbend Cellular Corp., Elkhart Cellular Telephone Company, Elkhart Metronet Inc., Lafayette Cellular Telephone Company, Mega Comm LLC, Michiana Metronet Inc., Southbend Metronet Inc.

² Because it only provides one category of service, Centennial only uses customer proprietary network information ("CPNI") to market various CMRS calling plans or CMRS features to customers who already purchase CMRS services from Centennial, which does not require customer approval under the CPNI rules (found at 47 C.F.R. § 64.2001 et seq., hereinafter "rules"). Centennial also does not disclose CPNI to, or permit access to CPNI by, third parties, except as may be required by law. For further discussion of Centennial's compliance with the CPNI rules, see Centennial's CPNI certification filed with the Commission on February 6, 2006.

customers to gain access to CPNI. Unfortunately, the rules being considered in this proceeding would, if adopted, do little if anything to alleviate the problem, while at the same time saddling the industry and consumers with cumbersome, static and ineffective security procedures.³ As a result, Centennial recommends that the Commission concentrate on the enforcement of its current rules and continuing the dialogue with industry, and decline to adopt the proposed rules.

I. THE PROPOSED RULES WILL NOT EFFECTIVELY ADDRESS THE PROBLEM OF PRETEXTING

The Commission launched this rulemaking to address concerns raised by the Electronic Privacy Information Center ("EPIC") regarding the illicit practice of pretexting, which involves data brokers gathering personal information about a customer from other sources (*e.g.*, the Internet) and then contacting the carrier pretending to be the customer in order to harvest CPNI.⁴ EPIC passingly acknowledges that the brokers are the real problem, but then quickly moves on to pointing fingers at the carriers, claiming that carriers' lax security measures are just as much to blame. The Commission initiated this rulemaking to consider whether the beefed up security measures suggested by EPIC would resolve the problem. The difficulty is that the proposed rules generally do not address the problem of pretexting and, to the extent that they do, they are unlikely to be very effective.

³ *In Re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, Notice of Proposed Rulemaking, 21 FCC Rcd 1782 (FCC rel. Feb. 14, 2006) (hereinafter "NPRM").

⁴ Of course, if a carrier's employee were to knowingly give CPNI to a data broker, that would clearly be a violation of current Commission CPNI rules, would simply be a matter of effective enforcement of those rules.

For example, EPIC has proposed that carriers be required to encrypt stored CPNI data.⁵ Encryption would protect the data against certain types of hacks into the carrier's computer systems. No one has suggested, however, that data brokers obtain CPNI by hacking into any carrier's database, and EPIC has failed to demonstrate how encryption would address the problem of which it complains. Moreover, carriers have a strong business interest in safeguarding their customers' personal information, and the current CPNI rules already impose a duty on carriers to protect this information. Imposing an encryption requirement would entail expensive and time-consuming upgrades to carriers' computer systems that would serve no purpose in this proceeding.

Another example is the proposal that carriers use customer-set passwords.⁶ EPIC would prefer carriers to use passwords rather than biographic identifiers because "unlike passwords, [biographic identifiers] . . . do not change, and they are widely available."⁷ Ideally, consumers *would* change their passwords often, and not use widely available words such as pet names or words appearing in the dictionary (which can be easily guessed through the use of hacking programs). In reality, consumers' practices fall far short of this ideal. Most use the same password or a few passwords for all situations and/or never change it, and many people continue to use dictionary words, pet names, etc. despite experts' warnings to the contrary.⁸ Moreover, passwords are not consumer-friendly. Centennial, like many other carriers, provides its customers with the option of

⁵ *In Re Implementation of the Telecommunications Act of 1996*, Petition of the Electronic Privacy Information Center for Rulemaking to Enhance and Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) (hereinafter "EPIC Petition") at 11; NPRM at ¶ 19.

⁶ EPIC Petition at 11; NPRM at ¶ 15.

⁷ EPIC Petition at 11.

⁸ See *Universal Authenticated Logon, A White Paper*, CRYPTOCARD Corp. at 1 (2003) available at <http://www.opsec.com/solutions/partners/downloads/cryptocard-whitepaper.pdf>; *Passwords: Why They Are So Easy to Crack*, Signify White Paper, available at <http://www.signify.net/uploads/Passwords-why-they-are-so-easy-to-crack.pdf> (last visited April 25, 2006).

using a password, but does not mandate passwords because most consumers find them burdensome. In response to a recent poll, most respondents (63%) said that it is inconvenient to have to remember passwords for these types of accounts and 42% said that they do not feel that using a password would increase their security.⁹ Passwords, in fact, may become outmoded as security needs increase while consumer tolerance for memorizing passwords decreases. Codifying a password requirement does not make sense in the quickly changing security environment in which carriers operate.

EPIC has also proposed new “audit trail” rules that would require carriers to record each time a customer’s record is accessed, whether information was disclosed and to whom.¹⁰ Customer service representatives (“CSRs”) already record this information under current telecommunications industry practices. For example, the computers used by Centennial’s CSRs automatically date and time stamp customer accounts each time they are accessed. This provides authorized law enforcement officials with the key information necessary to combat pretexting—the date and time that the pretexter obtained the information.¹¹ Given this, there is no need to impose new regulatory requirements to fix what isn’t broken. In fact, codifying the current practice could potentially impede carriers’ ability to quickly respond to new security threats by developing new CSR practices on an on-going basis.

EPIC has also proposed a new notice requirement under which carriers would notify customers of security breaches resulting in the unauthorized release of CPNI.¹²

⁹ *Ponemon Report, Those Pesky Passwords*, Larry Ponemon, CSO Online, March 2006, available at <http://www.csoonline.com/read/030106/ponemon.html?action=print>.

¹⁰ EPIC Petition at 11; NPRM at ¶ 17.

¹¹ The carrier’s records will show a contact with the (supposed) customer on a particular date and time at which, as the actual customer will explain, no real customer contact occurred. This will reveal which “customer” contact was actually contact by the pretexter.

¹² EPIC Petition at 11.

The Commission has also asked whether carriers should be required to provide notice of any and all releases of CPNI, even where there is no reason to suspect that the disclosure was illegitimate.¹³ There are several problems with these proposals. First, providing notice to customers in connection with routine, permissible disclosure of CPNI would impose major administrative burdens on carriers. Second, such notices would unnecessarily worry customers, many of whom will be bewildered by the receipt of multiple notices disclosing lawful activities of the carrier. Third, Congress is currently considering no less than three bills all proposing post-breach CPNI security notices.¹⁴ It would be premature for the Commission to impose such a requirement now.

Finally, EPIC suggests that older customer records should be destroyed when they are no longer needed for billing or dispute purposes.¹⁵ This is a solution in search of a problem. Nothing in the record indicates that the brokers are after older customer records, and carriers use historical calling records for a variety of legitimate reasons, sometimes years after the calls have been made. Similarly, “de-identifying” the records may impede carriers’ ability to settle disputes, or fully report information requested by law enforcement, which can also come years after a call is made. So, the Commission should reject these proposals as well.

II. THE COMMISSION SHOULD PREEMPT STATE CPNI LAWS AND REGULATIONS WITH RESPECT TO CARRIERS’ OBLIGATIONS

Many carriers, such as Centennial, offer multi-state or even nation-wide telecommunications services. Implementing, potentially, over fifty different state-level CPNI compliance programs, as well as a federal “overlay” scheme, is unworkable, overly

¹³ NPRM at ¶ 23.

¹⁴ See H.R. 4943, H.R. 4662 and S. 2389.

¹⁵ EPIC Petition at 11-12; NPRM at ¶ 20.

burdensome and unnecessary. Despite the fact that pretexting is already illegal under various state and federal consumer protection laws, there has been a recent flurry of state legislative activity to explicitly prohibit the practice. Interestingly (and appropriately), most of this state legislative activity is aimed at the pretexters, and not carriers. Thus, it seems that most states recognize that it is the pretexters' behavior that needs to be addressed, and that the current federal CPNI rules are sufficient for regulating carriers' behavior. Several states, nonetheless, have proposed legislation that regulates carriers' behavior. The Georgia legislature, for example, has passed a bill that would make it a felony for any employee, officer, etc. of a mobile telephone service provider to disseminate customers' telephone records to specifically-named entities and persons, such as affiliates or agents, without customer consent. The legislation contains a global exception, however, that "such information may be provided to such subscriber in the normal course of business."¹⁶ This legislation differs from the federal rules (both current and proposed). Particularly given that Georgia seeks to impose criminal liability on carriers and other states may follow suit, it is imperative that the Commission preempt the states and give carriers one set of clearly-stated, nationally-applicable rules to follow.


III. CONCLUSION

As discussed above, the CPNI rules proposed by EPIC fail to address the problem of pretexting, principally because they are not directed at the offending parties—the pretexters. Codifying static security mandates that fail to effectively address the problem will only serve to increase carriers' costs and detract from resources that could be used by the industry to respond to the ever-evolving security environment. The solution to the pretexting problem lies in continuing enforcement of the current rules, coupled with

¹⁶ Georgia S.B. 456 at (c).

cooperation between the Commission, the industry and consumers to achieve the common goal of battling the pretexters. Carriers such as Centennial have a strong business interest in protecting their customers' CPNI, and Centennial makes continual improvements to its security procedures. That business interest is best served by giving carriers the flexibility to quickly respond to new security threats, unhampered by static regulatory requirements. Centennial therefore respectfully requests that the Commission decline to adopt EPIC's proposed new rules, and preempt the states from imposing a patchwork of inconsistent rules.

Respectfully submitted,



Christopher W. Savage

Danielle Frappier

Cole Raywid & Braverman, LLP

1919 Pennsylvania Ave., NW, Suite 200

Washington, D.C. 20006

(202) 659-9750

csavage@crblaw.com; dfrappier@crblaw.com

**Counsel for Centennial Communications
Corp.**

William Roughton
Vice President, Legal and Regulatory
Affairs
Centennial Communications Corp.

Of Counsel

April 28, 2006